must also contain operational recommendations for responding to the data breach. Each risk analysis, regardless of findings and operational recommendations, shall also address all relevant information concerning the data breach, including the following:

(a) Nature of the event (loss, theft, unauthorized access).

(b) Description of the event, including:

(1) Date of occurrence;

(2) Data elements involved, including any personally identifiable information, such as full name, social security number, date of birth, home address, account number, disability code;

(3) Number of individuals affected or potentially affected;

(4) Individuals or groups affected or potentially affected;

(5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

(6) Time the data has been out of VA control;

(7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons); and

(8) Known misuses of data containing sensitive personal information, if any.

(c) Assessment of the potential harm to the affected individuals.

(d) Data breach analysis, as appropriate.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.116 Secretary determination.

(a) Upon receipt of a risk analysis prepared under this subpart, the Secretary will consider the findings and other information contained in the risk analysis to determine whether the data breach caused a reasonable risk for the potential misuse of sensitive personal information. If the Secretary finds that such a reasonable risk does not exist, the Secretary will take no further action under this subpart. However, if the Secretary finds that such a reasonable risk exists, the Secretary will take responsive action as specified in this subpart based on the potential harms to individuals subject to a data breach.

(b) In determining whether the data breach resulted in a reasonable risk for the potential misuse of the compromised sensitive personal information, the Secretary shall consider all factors that the Secretary, in his or her discretion, considers relevant to the decision, including:

(1) The likelihood that the sensitive personal information will be or has been made accessible to and usable by unauthorized persons;

(2) Known misuses, if any, of the same or similar sensitive personal information;

(3) Any assessment of the potential harm to the affected individuals provided in the risk analysis;

(4) Whether the credit protection services that VA may offer under 38 U.S.C. 5724 may assist record subjects in avoiding or mitigating the results of identity theft based on the VA sensitive personal information that had been compromised;

(5) Whether private entities are required under Federal law to offer credit protection services to individuals if the same or similar data of the private entities had been similarly compromised; and

(6) The recommendations, if any, concerning the offer of, or benefits to be derived from, credit protection services in this case that are in the risk analysis report.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.117 Notification.

(a) With respect to individuals found under this subpart by the Secretary to be subject to a reasonable risk for the potential misuse of any sensitive personal information, the Secretary will promptly provide written notification by first-class mail to the individual (or the next of kin if the individual is deceased) at the last known address of the individual. The notification may be sent in one or more mailings as information is available and will include the following:

(1) A brief description of what happened, including the date[s] of the data breach and of its discovery if known;

(2) To the extent possible, a description of the types of personal information that were involved in the data breach (e.g., full name, Social Security

number, date of birth, home address, account number, disability code);

(3) A brief description of what the agency is doing to investigate the breach, to mitigate losses, and to protect against any further breach of the data;

(4) Contact procedures for those wishing to ask questions or learn additional information, which will include a toll-free telephone number, an e-mail address, Web site, and/or postal address;

(5) Steps individuals should take to protect themselves from the risk of identity theft, including steps to obtain fraud alerts (alerts of any key changes to such reports and on demand personal access to credit reports and scores), if appropriate, and instruction for obtaining other credit protection services offered under this subpart; and

(6) A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system.

(b) In those instances where there is insufficient, or out-of-date contact information that precludes direct written notification to an individual subject to a data breach, a substitute form of notice may be provided, such as a conspicuous posting on the home page of VA's Web site and notification in major print and broadcast media, including major media in geographic areas where the affected individuals likely reside. Such a notice in media will include a toll-free phone number where an individual can learn whether or not his or her personal information is possibly included in the data breach.

(c) In those cases deemed by the Secretary to require urgency because of possible imminent misuse of sensitive personal information, the Secretary, in addition to notification under paragraph (a) of this section, may provide information to individuals by telephone or other means, as appropriate.

(d) Notwithstanding other provisions in this section, notifications may be delayed upon lawful requests, from other Federal agencies, for the delay of notifications in order to protect data or computer resources from further compromise or to prevent interference with the conduct of an investigation or efforts to recover the data. A lawful request is one made in writing by the entity or VA component responsible for the investigation or data recovery efforts that may be adversely affected by providing notification. Any lawful request for delay in notification must state an estimated date after which the requesting entity believes that notification will not adversely affect the conduct of the investigation or efforts to recover the data. However, any delay should not exacerbate risk or harm to any affected individual(s). Decisions to delay notification should be made by the Secretary.

(Authority: 38 U.S.C. 501, 5724, 5727)

§ 75.118 Other credit protection services.

(a) With respect to individuals found under this subpart by the Secretary to be subject to a reasonable risk for the potential misuse of any sensitive personal information under this subpart, the Secretary may offer one or more of the following as warranted based on considerations specified in paragraph (b) of this section:

(1) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

(2) Data breach analysis;

(3) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution; and/or

(4) One year of identity theft insurance with $20,000.00 coverage at $0 deductible.

(b) Consistent with the requirements of the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*) as interpreted and applied by the Federal Trade Commission, the notice to the individual offering other credit protection services will explain how the individual may obtain the services, including the information required to be submitted by the individual to obtain the services, and the time period within which the individual must act to take advantage of the credit protection services offered.

(c) In determining whether any or all of the credit protection services specified in paragraph (a) of this section will be offered to individuals subject to a